IN THE CLAIMS

Listing of the Claims

1. (Previously presented) A method comprising:
storing a private key associated with a user at an authentication server;
receiving a request for access to a service from the user ;
collecting a biometric sample from the user via a client associated with the user and remote from the authentication server on a network;
sending the collected biometric sample from the client to the authentication server;
comparing, at the authentication server, the biometric sample to a biometric template associated with the user; and
if a result of the comparing step indicates a match between the biometric sample and template for the user:
allowing the private key from the authentication server to be accessed and used with the request;
encrypting the request with the private key, and
providing the service with access to a public key corresponding to the private key,
wherein access to the private key stored at the authentication server for use in encrypting the user's request is prevented unless and until the authentication server determines that the user's collected biometric sample that was sent by the client matches the biometric template.

2. (Previously presented) A method according to claim 1, further comprising:
if the result indicates a match, generating a digital signature using the private key for use with the request.

3. (Original) A method according to claim 2, further comprising:
providing the digital signature to the service associated with the request.

4. (Original) A method according to claim 1, further comprising:
providing a biometric signature corresponding to the collected biometric sample to the service associated with the request.

5. (Original) A method according to claim 4, further comprising:
allowing the service to determine whether to fulfill a transaction corresponding to the request in accordance with the result of the comparing step.

6. (Original) A method according to claim 1, further comprising:
generating pre-enrollment keys for the user;
supplying the pre-enrollment keys to respective key generators; and
generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators.

7. (Original) A method according to claim 6, further comprising:
verifying registration of the user in accordance with a comparison of the final enrollment key;
creating the biometric template for the user only if registration is verified; and
generating the private key only if the biometric template is successfully created.

8. (Original) A method according to claim 6, further comprising associating user identification information with the final enrollment key.

9. (Previously presented) A method according to claim 1, further comprising:
encrypting the collected biometric sample for transmission to the authentication server; and
including integrity information in the encrypted biometric sample.

10. (Original) A method according to claim 9, further comprising:
decrypting the encrypted biometric sample at the authentication server; and
checking the integrity information included with the biometric sample.

11. (Original) A method according to claim 9, wherein the integrity information includes a unique transaction identifier.

12. (Previously presented) A method according to claim 1, further comprising:
associating user identification information with the private key; and
maintaining a digital certificate containing the user identification information and the public key corresponding to the private key at the authentication server.

13. (Original) A method according to claim 1, wherein the biometric sample includes a fingerprint scan.

14. (Previously presented) An apparatus comprising:
means for storing a private key associated with a user at an authentication server;
means for receiving a request from the user for access to a service;
means for collecting a biometric sample from the user via a client associated with the user and remote from the authentication server on a network;
means for ending the collected biometric sample from the client to the authentication server;
means for comparing the biometric sample to a biometric template associated with the user; and
if a result of the comparing means indicates a match between the biometric sample and template for the user:
means for allowing the private key from the authentication server to be accessed and used with the request;
means for encrypting the request with the private key, and
means for providing the service with access to a public key corresponding to the private key,
wherein access to the private key stored at the authentication server for use in encrypting the user's request is prevented unless and until the authentication server determines that the user's collected biometric sample that was sent by the client matches the biometric template.

15. (Previously presented) An apparatus according to claim 14, further comprising:
if the result indicates a match, means for generating a digital signature using the private key for use with the request.

16. (Original) An apparatus according to claim 15, further comprising:
means for providing the digital signature to the service associated with the request.

17. (Original) An apparatus according to claim 14, further comprising:
means for providing a biometric signature corresponding to the collected biometric sample to the service associated with the request.

18. (Original) An apparatus according to claim 17, further comprising:
means for allowing the service to determine whether to fulfill a transaction corresponding to the request in accordance with a result of the comparing means.

19. (Original) An apparatus according to claim 14, further comprising:
means for generating pre-enrollment keys for the user;
means for supplying the pre-enrollment keys to respective key generators; and
means for generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators.

20. (Original) An apparatus according to claim 19, further comprising:
means for verifying registration of the user in accordance with a comparison of the final enrollment key;
means for creating the biometric template for the user only if registration is verified; and
means for generating the private key only if the biometric template is successfully created.

21. (Original) An apparatus according to claim 19, further comprising means for associating user identification information with the final enrollment key.

22. (Previously presented) An apparatus according to claim 14, further comprising:
means for encrypting the collected biometric sample for transmission to the authentication server; and
means for including integrity information in the encrypted biometric sample.

23. (Original) An apparatus according to claim 22, further comprising:
means for decrypting the encrypted biometric sample at the authentication server; and
means for checking the integrity information included with the biometric sample.

24. (Original) An apparatus according to claim 22, wherein the integrity information includes a unique transaction identifier.

25. (Previously presented) An apparatus according to claim 14, further comprising:
means for associating user identification information with the private key; and
means for maintaining a digital certificate containing the user identification information and the public key corresponding to the private key at the authentication server.

26. (Original) An apparatus according to claim 14, wherein the biometric sample includes a fingerprint scan.

27. (Withdrawn) An authentication infrastructure comprising:
a server that intercepts a request by a user for access to a service and controls access to a stored private key associated with the user; and
a client that collects a biometric sample from the user in response to the user making the request and sends the collected biometric sample to the server,
wherein the server maintains a biometric template associated with the user for authenticating the collected biometric sample, and
wherein, if and only if the collected biometric sample matches the biometric template:
the server allows access to the stored private key for use in encrypting the request, so that the user need not maintain a token for accessing the service, and the user need not store the private key, and

the server provides the service with access to a public key corresponding to the private key,

wherein access to the private key stored at the server for use in encrypting the user's request is prevented unless and until the authentication server determines that the user's collected biometric sample that was sent by the client matches the biometric template.

28. (Withdrawn) An authentication infrastructure according to claim 27, wherein the private key is further used to sign a message for allowing the user to perform the transaction with the service, the service obtaining the corresponding public key from the server.